Sub C1

CLAIMS

1. Process for the remote authentication of a user (7) for local access to a local machine (4) belonging to a network (5) that includes a remote server (3) managed by an administrator (8) and containing means (6) for classifying information, characterized in that it consists of:

- creating a challenge (D) capable of being transmitted by communication means (9), the communication means (9) connecting the user (7) with the administrator (8);
- communicating to the administrator (8) the challenge (D) created as well as elements known by the user, via the communication means (9);
- performing a predetermined calculation by means of the server (3) in order to obtain a response (RD) that is a function of the challenge (D) and/or of predetermined data;
- transmitting to the user (7) the response (RD) obtained through the communication means (9);
- performing a calculation by means of the local machine (4) in the same way as the server (3) in order to obtain a response (RD1) that is a function of the challenge (D) and/or of predetermined data;
- comparing the response (RD) transmitted by the administrator to the response (RD1) calculated by the local machine (4) and locally authorizing the user's connection to the machine (4) based on the result of the comparison.

B

2. Process according to claim 1, characterized in that the calculation performed by the server (3) consists of modifying, in accordance with a given algorithm, the challenge (D) and/or at least one of the following pieces of data: at least one piece of information issued by the classification means and known by the user, at least one secret shared between the server (3) and the local machine (4), at least one element communicated by the user.

3. Process according to either of claims 1 or 2, characterized in that the calculation performed by the local machine (4) consists of modifying, in accordance with a given algorithm, the challenge (D) and/or at least one of the following pieces of data: at least one secret shared between the server (3) and the local machine (4), at least one element communicated by the user.

4. Process according to either claim 2 or 3, characterized in that the shared secrets are entered into the server (3) and transmitted to the local machine (4) during a successful network authentication.

5. Process according to any of claims 2 through 4, characterized in that the shared secret or secrets are modified by means of a modification key (C) that depends on the local machine (4), prior to being modified by the algorithm.

6. Process according to claim 5, characterized in that the modification key (C) consists of concatenating the secret or a combination of secrets existing in the form of a byte string called a Master Station Secret and of hashing the byte string obtained through concatenation by means of a calculation algorithm, in order to obtain a byte string called a Station Secret.

7. Process according to any of claims 2 through 6, characterized in that the shared secret or secrets are accompanied by a version number that is incremented each time the secret is modified.

8. Process according to any of claims 1 through 7, characterized in that the challenge is constituted by a byte string.

9. Process according to claims 7 and 8, characterized in that the challenge is composed of:

- a first byte representing the type of challenge, the type indicating whether a network authentication has been performed;
- second and third bytes representing the version number of the shared information;
- random alphanumeric characters of the fourth to twelfth bytes.

10. Process according to claim 6, characterized in that the response (RD; RD1) is calculated by hashing, in accordance with a calculation algorithm, a character string

composed of the concatenation in a predetermined order of the challenge, the character string resulting from the transformation by a calculation algorithm of the user's password, the Station Secret and the user's name.

11. Process according to any of claims 1 through 9, characterized in that the response (RD; RD1) is calculated by hashing, in accordance with a calculation algorithm, a character string composed of the concatenation in a predetermined order of the challenge, a fixed security key CC stored in the local machine (4) and in the server (3), the name of the local machine (4), the character string resulting from the transformation by a calculation algorithm of the user's password and user name.

12. Process according to any of claims 1 through 11, characterized in that the local connection authorized is temporary, the authorized duration being configurable.

13. Process according to any of claims 1 through 12, characterized in that it consists of locally authenticating the user (7) after a disconnection by the user (7) authenticated remotely.

14. System for the remote authentication of a user (7) for local access to a machine called a local machine (4) belonging to a network (5) that includes a remote server (3) managed by an administrator (8) and containing means (6) for classifying information, characterized in that it comprises communication means (9) connecting the user (7) with the administrator (8), in that each local machine (4) comprises a user authentication module (10) that includes a user module for generating a challenge (11) and a user module for calculating a response to a challenge (12), and in that the server (3) comprises an administrative authentication module (13) comprising an administrative module for calculating a response to a challenge (14).